Scientific Research Publishing

Open Journal of Social Sciences, 2020, 8, 231-241
https://www.scirp.org/journal/jss
ISSN Online: 2327-5960
ISSN Print: 2327-5952

Analysis of the Problems of Ensuring Information Security in the Terms of the Contemporary Society

Dmitrii S. Brazevich[1*], Zhanna S. Safronova[2], Tatyana N. Kosheleva[1], Alla V. Biryukova[1]

[1]Saint-Petersburg University of Civil Aviation, St.-Petersburg, Russia
[2]Saint Petersburg State Chemical and Pharmaceutical University, St.-Petersburg, Russia
Email: *brazevich1986@mail.ru

How to cite this paper: Brazevich, D. S., Safronova, Z. S., Kosheleva, T. N., & Biryukova, A. V. (2020). Analysis of the Problems of Ensuring Information Security in the Terms of the Contemporary Society. *Open Journal of Social Sciences, 8,* 231-241.
https://doi.org/10.4236/jss.2020.82018

Received: May 7, 2019
Accepted: February 25, 2020
Published: February 28, 2020

Abstract

The article analyzes the domestic and foreign experience of information security in today's society. The peculiarities of the research are analyzing the process of information security from the point of two sociological paradigms: structural-functional and interpretive. The process of informatization in the society is one of the key factors of its development. This article analyzes the establishment of an information society. The article analyzes the process of informatization, which is to facilitate the survival of humanity and set it on the path of sustainable development. Owing to that fact, the problem of information security is attracting increasing interest; it is assuming primary importance among the rest of security types. This problem is investigated with the following methods. First, we reveal the nature of information security, its forms, and content within the framework of the modern information society. Second, we define the possible ways information security affects the development of society.

Keywords

Information, Information Society, Information Sphere, Information System, Information Security, Communication, Information Risk, Structural-Functional Analysis, Sociological Paradigm

1. Introduction

The issue of information security is arising under the conditions of informatization, which is going global in the XXI century. The study of modern positive and negative development trends of informatization process and forecasting its fu-

ture development trends have been gaining importance in recent years.

In the first case, the development of informatization cannot be entirely secure for an individual, society, government, or world community. The information trends that correspond to the principles of sustainable development and will be retained in a new civilization development pattern are the following: the increase of informational needs of an individual and society; the transformation of information into a resource that is setting the further development for civilization; the systematic character of informatization; the intellectualization and virtualization of society; the establishment of information sphere; information security ensuring; the formation of the global knowledge bank and the integral intelligence of humanity, the establishment of the information society.

Nowadays, ensuring information security is considered to be a very complicated, multifunctional process that depends on various internal and external factors. The main reason for this is that the present stage of social development is related to the assimilation and implementation of opportunities in the information sphere, such as network communication, biorobotics, etc.

2. Information Security Analysis

Creation of information society in Russia is associated with the emergence of a number of key problems, on the decision of which the quality of life of the society as a whole depends. Analysis of the development of informatization in Russia makes it possible to highlight the security problem as one of the problems of the formation of the Information Society.

Nowadays researchers are beginning to study information security in the context of the socio-cultural life of society, and the whole area of knowledge associated with the functioning of various social institutions remain poorly researched.

All the variety of approaches to information is determined by the specifics of the fields in which this concept is used. The difference in the way information is transmitted, the types of information threats and the forms of presentation of finished information products generate different views on the study of key aspects of information security.

3. Sociological Approach of Information Security

Information security within the framework of sociological approach is considered as subject to the preservation of the social component of the dynamic stability of the system. In N.V. Lopatina's opinion any information technology cannot be considered as a non-social phenomenon: like the technology of any kind, information technology acts as a product of human activity, focused on the search for new tools, forms and methods of transformation of reality, and aimed social needs. According to N.V. Lopatina, information technology is the product of social experience [(Lopatina, 2006: p. 17)]. Information security can be implemented exclusively in the field of social relations and, like any social pheno-

menon, is the subject to sociological study in order to obtain data on the social system (field of information functioning) and its response to the recipient.

3.1. Information Technology as a Part of the Organization

In modern conditions, one of the driving forces of the development of society is the use of information technology. Information systems have become an integral part of the structure of any organization. They allow better information exchange, facilitate work with foreign partners and are necessary when building relations within society.

Experience shows that when problems arise in the information exchange system, the organization is on the verge of dysfunction. Therefore, representatives of public and business structures are aware of the importance of ensuring the security of information resources, making them an integral part of the development strategy of the organization and society as a whole. The urgent need for information security has an impact on the development of technical means of protecting, as well as rethinking the attitude to this problem from the point of view of its socio-cultural influence on society.

3.2. Social and Cultural Aspects of Information Security

Nowadays most researchers consider information security as a complex problem, and the technological aspect gradually fades into the background, giving priority to the social and cultural aspects. The formulation of this trend is due to the fact that in the process of information exchange leading role belongs to man – the carrier and user of information and knowledge. Efficiency and reliability of the information-oriented system depend on how much interests and psychological features of personality will be taken into account in the process of information exchange.

Thus, nowadays information security is a comprehensive data protection on the state and movement of tangible and intangible assets, their processing and transmission. It is also protection of information carriers, storage means IT-systems, and, in addition, ensuring the protection on the vital interests of the individual, society and the state against intentional or unintentional influences in this or that form on the scope of information.

Unfortunately, today there are practically no poliparadigmal studies of the problem of information security, which would take into account the sociological aspect. The purpose of this article is to study the issue of ensuring information security in terms of two sociological paradigms. According to professor G. Dillon, Director of the Institute of Information Technology, and Professor J. Backhouse, Director of Integrity Group, "it is important to understand the conceptual foundation of various approaches to security" [(Dhillon & Backhouse, 2001: p. 128)]. As it is known, in 1979 G. Burrel and G. Morgan developed a model of four sociological paradigms (Burrell & Morgan, 1979). This model allows researchers to understand what underlies the various concepts of information se-

curity, primarily to its sociological aspect. G. Burrel and G. Morgan created their own conceptual and technological system in which two sets of theories (depending on the orientation to subjective and objective factors) were singled out.

The objectivist position is that the world is seen as external to the individual. This "external" world is real, has a clearly defined structure with certain functions and exists independently of the person; nominalists (or subjectivists) perceive the reality as the result of individual cognition. The individual creates the world and calls its concrete phenomena to give the world meaning and establish the interaction of individuals. The nominalists believe that objectivists make a serious mistake when perceiving metaphors literally and turning constructs into something concrete. In their turn, the objectivists believe that the mistake of the nominalists is in their ignoring these constructs.

3.3. Sociological Paradigms of Studying Information Security

According to G. Burrel and G. Morgan researchers focus on studying the need to regulate human relations, which is an important aspect of comprehensive information security. The main question that these researchers try to answer is understanding the society as a system, as a single organism, as the organization [5, p. 17]. It is within the framework of this paradigm that many aspects of information security are studied. The method of check-lists, risk analysis, and assessment was developed among other things. Check-lists are used to identify all possible options for monitoring information. The purpose of this technique is to study the entire spectrum of security-related system elements for developing an "ideal", "invulnerable" system (Baskerville, 1993). In other words, check-lists provide the definition and choice of the optional way of achieving specific goals. Despite the fact that the method of checklists is quite widespread in the field of information security, its drawback lies in the fact that it pays more attention to procedures relating to solving specific problem situations than to investigating the social nature of these problems. Check-lists encourage the analysis of procedures without discussing the problem (because of which these procedures actually appeared) and possible outcomes. It is understood that the purpose was agreed in advance.

Another category of functionalist paradigm is the category of risk. Analysis of the risk system is a very important tool for ensuring information security because it structures and organizes the whole process, which contributes to the development and reliable system of protection of the organization. An essential part of the risk analysis system is the correct identification of existing risks and the search for ways to minimize them. The main factors of risky behavior include social (associated with the influence of the media and national culture on the risky consciousness of public opinion), organizational (organizational-technological, ergonomic and management factors) and socio-psychological factors (associated with the influence of other people on the risky behavior of a person and the degree of his involvement in joint activities), as well as specific

features of the tasks to be solved (associated with the problem of choice and the presence of danger).

One of the most significant factors determining the reliability of the system is a person. None of the existing automated systems, no matter how perfect it may seem, can function properly without human control. Information management and related management practices of information security and risk minimization acquire special significance. From the point of view of risk management, information management determines the behavior of the individual in the event of a non-regular situated considered as an information threat. Research in this area is still under development.

However, it has already become apparent that the analysis itself will change in the process of solving problems related to risk management in the new environment, as well as ensuring security through synergistic methods and methods of nonlinear dynamics. Such an approach will increase the effectiveness of preventing the emergence of new risks in the field of information security significantly.

But, at this stage of development, risk analysis has several drawbacks. Thus, the classical probability theory is not suitable for assessing security risks, because the mechanism of the emergence of threats does not yield to any forecasting, is chaotic. In addition, risk analysis is too simple a technique. It defines the organization in terms of assets (basically it is about information, hardware, and software), but does not survey the society and simply identifies and assesses risk factors or conducts diagnostics of group behavior.

Another area of functionalist research is the study of security policies. They proposed a variety of options for such structures in an attempt to help formulate the concept of ensuring information security for privacy. Van den Hoven considers privacy as a human right, in the sense of protecting people' intrinsic value:

- Prevention of information-based harm;
- Prevention of information inequality;
- Prevention of information injustice and dis-crimination;
- Safeguarding autonomy [(Wolter Pieters, 2017: p. 278)].

For example, N. Kolokotronis and his group put forward a multilevel and multidimensional model consisting of such phases as analysis/verification of the needs of the organization; the study of risks and evaluation of their costs; the development of a security strategy; monitoring the results of the latter [(Kolokotronis, 2002: p. 166)]. Researchers emphasize that the problem of information security should be the subject of special attention at the highest level of management of an organization and cannot be perceived as a private technical task (or a number of tasks) associated with solving specific problems. They noted the change in the attitude of scientists and practitioners to the problem of ensuring information security, their understanding that it concerns not only the development and implementation of software and hardware but is also an actual socio-cultural problem of our time, the ignoring of which can provoke cata-

strophic consequences for society as a whole.

When investigating the problem of information security, functionalists came to the conclusion that the environment of various organizations has the same characteristics as the physical world. This allowed them to put a scientific foundation under the concept of information security and management. Managers, in this case, were perceived as a product of their own environment. Communities, organizations and control systems appeared to be independent of individual cognitive ability. According to functionalists, this leads to the fact that managers tend to concentrate on the needs and objectives of the organization in developing a strategy to ensure information security. Moreover, managers view information as giving a comprehensive picture of reality and, therefore, try to satisfy the designated needs with it. Functionalists also came to the conclusion that provided that all subsystems work efficiently, the organization is almost completely protected from risks.

Functionalists proposed their own way of ensuring information security. According to it, the organization that ensures the security of subsystems ensures its security in general. In this case, various parts of the system that guarantee a sufficient level of security to individual units are not interdependent. Thus, overall security can be ensured by examining the mechanism of action of the various components of the system carefully. However, in the process of such an analysis, hidden feelings, attitudes and perceptions of information security may remain undetected.

3.4. Interpretive Paradigm

Both researchers who adhere to the interpretive paradigm and functionalists agree that the principle of regulation and stability is effective and important. Nevertheless, representatives of the interpretive approach consider problems from the personal point of view, they are interested in the subjective perception of certain social situations that exists in each individual. It is possible to note the study of I. Koskosas and R. Paul, who used the socio-organizational direction for research on the security of information systems. They have developed a concept that illustrates three such components as trust, culture, and communication about risks in defining the objectives of the security systems (Koskosas & Paul, 2003).

Risk analysis was also actively discussed in the framework of this paradigm. For example, L. Willcocks and H. Margetts used a model to assess the degree of risk threatening the information system that emphasizes the value of historical, procedural and content analyzes and noted the importance of social and qualitative characteristics of information security (Willcocks & Margetts, 1994). U. Beck and R. Baskerville criticized the functionalist approach to researching risks. They considered it unjustified, on one hand, to attach great importance to technical devices that increase the security of the information system and, on the other hand, to ignore such factors as people's understanding of the goals and motives of their actions. U. Beck pointed out that risks in a developed market

society cannot be taken unambiguously, because "the risks here are not only risks but also market chances" [(Beck, 2000: p. 56)]. R. Baskerville argued that risk analysis becomes more effective and valuable when used as a communication tool, especially between security professionals and supervisors. Models of business management and information security of the organization were developed using the tools of this interpretive paradigm [(Baskerville, 1991: p. 121)].

3.5. Negative side of Information Society

A. J. Schereder, A. Deursen investigate negative outcomes of Internet use in the way of interpretive paradigm. These outcomes have different types as economic, cultural, social, personal consequence. Economic outcomes of Internet use often associated with specific activities, such as online shopping, gambling. Such activities lead to debt, financial fraud.

Negative cultural outcomes of Internet use relate to an individual norms and behavior and correspond with the identity and belonging categories in cultural field. For instance, in Russia we have traditional culture and subculture. Youth identificated yourself with subculture get tattoo, which can cause different problems with health, even infects aids.

Other activities regarded as cybercrime include identity theft, phishing, and cyberbulling on social media. Negative outcomes in cultural field can evoke sadness, anxiety and irritability. Other studies indicate that social media use leads to neglect of social activities, choosing social media and smartphones to real-life relationships, and the weakening of existing social ties.

Negative consequence of personal field are often associated with the individuals' mental or physical state, such as aggression and hostility, neglect of health, changes in sleep and eating patterns, anxiety, and reducing of other pastime activities.

There are different strategies to cope with negative outcomes of Internet use. Examples include seeking friends and family support, ignoring persons who send offensive messages, and blocking certain Web sites in the case of privacy concerns [(Scheerder et al., 2019: p. 413)].

Russian sociologists highlight features inherent in the information society, such as:

- computer gambling;
- general mobility of the population;
- a great distance between youth and old generation.

The digital inequality every year significantly increasing in Russia, that is why the government is trying to regulate information issues. Information technologies change the amount of effort required for certain actors to access certain information and thereby enable social transformation [(Janitsky, 2016: p. 94)].

3.6. Ensuring Information Security

D. Backhouse and G. Dillon created a model of information security, taking into

account the factor of internal non-obvious patterns of behavior of members of the organization. This discovery allowed the authors to simulate the behavior of people in situations where it is necessary to act in a coordinated manner. The interaction of the members of the organization was discussed at the level of ensuring general information security [6].

B. von Solms, for example, stressed that "if information security is not given the most serious importance at the level of the organization, if all levels and dimensions are not taken into account, then with 100% probability, sooner or later, there will be real threats to the existence of the organization itself" [(Von Solms, 2001), p.504]. From the point of view of B. von Solms, the issue of ensuring information security is not a technical problem exclusively. Such components as the management, cultural and structural characteristics of the organization can make a difference. Decisions concerning society must precede decisions regarding the technical aspect of security. Technical solutions should be a support and stimulus for the desired behavior of people who make up this community.

According to Isto Huvila (2018) almost all information is produced using digital devices and they have replaced a large number of nondigital measurement, documentation, and information processing instruments [(Isto Huvila, 2018: p. 229)].

In Russia elderly people, have difficulties with using Internet, smartphones, ATMs and other devices. The government allocates large amounts of money to train elderly people to use information technology, as the media environment has developed widely in large metropolitan areas.

In our opinion, consideration of the issue of ensuring information security from the standpoint of the interpretive paradigm allows, firstly, to consider the problem as complex and systemic; secondly, to identify and analyze human behavior and mechanisms of interactions; and, thirdly, to combine the study of technical and human factors in the investigated process. Within the framework of this paradigm, information security is considered and studied in terms of the contextual perspective and to take into account the human factor. Among the potentially promising areas of research is the perception of risks, people's responsibility for their behavior, and the emergence and evaluation of its informal norms.

Most Russian organizations prefer multi-level methods of work that turn the information system into an integral part of the organization activities. The need to go beyond the strict framework of the functionalist paradigm allows studying the interaction between people, their behavior patterns, contradictions, meanings, associated with this or that action. In other words, scientists will have to study the problem of ensuring information security in a complex way, using the methods of interpretive paradigm. For those, who have already used these tools, it is obviously useful to take advantage of the achievements of such social theories as phenomenalism, hermeneutics and the theory of conflict. It should be

noted that researchers have discovered the advantages and disadvantages of each paradigm long ago, making it possible to create the most effective scheme for ensuring information security.

4. Conclusion

This paper gives a view of ensuring information security so that we can understand the methods of analyzing information security more clearly. Proponents of the use of more traditional positivist methods of analyzing of information security prefer using the existing scheme for studying various data. They do not investigate the problem in a broad context that includes organizational culture, requirements for the level of competence of ordinary employees, formal and informal relations, changes connected with personal relationships of individuals and so on.

As consequence positivists do not always capture and correctly interpret many interesting and important aspects of the research project. They perceive information security as a purely scientific or technical problem.

The interpretive approach emphasizes the importance of the socio-technical nature of information systems. It pays attention to objectives related to the organizational and social context, with the need to share information, empowerment, creativity and innovation, and motivation of staff.

Within the framework of the traditional positivistic analysis, it has been accepted that people tend to communicate and establish relationships. And within the framework of the interpretive approach, it is important to understand what people are establishing communication about and how they interact in the organizational context. Positivists focus on solving the problem of information security, while supporters of the interpretive paradigm focus on a deeper understanding of the problem and its various aspects (Trauth & Jessup, 2000).

Traditional analysis, such as check-list or risk analysis, is more suitable for studying problems when there is confidence in the existence of a universal correct solution. Interpretive analysis is suitable for studying problems that are not fully understood yet or have an emotional component, and in the case when the organization is of a political nature.

As a result, interpretive studies expand the area of analyzes, including such factors as organizational context, the interaction between people, communication, behavior, roles, emotions, and actions.

Social transformation into an information society in Russia has special features determined by the specific character of modern mass media performance, the peculiarity of state legal system, as well as social, cultural and psychological factors of social and individual minds. In the establishment of the information society, the government coordinates various social subjects' activities. It aims at encouraging people to integrate into a new technological environment with a deliberate policy, developing the branches of information industry, ensuring democracy progress and observance of individual rights.

The correlation of economic, social, cultural and technological factors in the establishment of an information society reveals itself in the liberalization of mass media functioning rules, forming new requirements for journalists, and a growing role of state regulation. It has been demonstrated that the tendency for building an information society in the regions of the Russian Federation is based mainly on the successful development of informational and telecommunicational technologies and on the considerable government support for these innovations. The relation between the successful establishment of an information society and the information sphere, which contains traditional structures and relationships that were modernized and acquired new integral functions, has been found.

So, we must state that each paradigm has its advantages and disadvantages. But applying the theoretical and methodological synthesis, which uses the developments of various sociological paradigms (in which the problems of information security are investigated), there is always an opportunity to conduct research and to understand the complexity of the problem of ensuring information security in the conditions of modern society.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

Baskerville, R. (1991). Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security. *European Journal of Information Systems, 1,* 121-130. https://doi.org/10.1057/ejis.1991.20

Baskerville, R. (1993). Methods of the Organization of Information Systems. *Computer Studies, 25,* 375-414. https://doi.org/10.1145/162124.162127

Beck, U. (2000). *Risk Society. On the Way to Another Modern*. M.: Progress-Tradition.

Burrell, G., & Morgan, G. (1979). *Sociological Paradigms and Organizational Analysis*. London: Heinman.

Dhillon, G., & Backhouse, J. (2001). Current Directions in IS Security Research: Towards Socio-Organisational Perspectives. *Information Systems Journal, 11,* 127-153. https://doi.org/10.1046/j.1365-2575.2001.00099.x

Huvila, I. (2018). Putting to (Information) Work: A Stengersian Perspective on How Information Technologies and People Influence Information Practices. *The Information Society, 34,* 229-243. https://doi.org/10.1080/01972243.2018.1463332

Janitsky, O. N. (2016). Information Society: Problems and Methods of Their Solution. *Power, 7,* 90-96.

Kolokotronis, N., Margaritis, C., Papadopoulou, P., Kanellis, P., & Martakos, D. (2002). An Integrated Approach for Securing Electronic Transactions over the Web. *Benchmarking: An International Journal, 9,* 166-181. https://doi.org/10.1108/14635770210421836

Koskosas, I., & Paul, R. (2003). The Performance of Risk Management in the Context of Goal Setting: The Case of Internet Banking. In T. Acton (Ed.), *Proceedings of the 8th Collaborative Electronic Commerce Technology and Research Conference* (pp.

242-249).

Lopatina, N. V. (2006). *Information Specialists: Sociology of Management* (208 p.). M.: Academic Project.

Pieters, W. (2017). Beyond Individual-Centric Privacy: Information Technology in Social Systems. *The Information Society, 33,* 271-281. https://doi.org/10.1080/01972243.2017.1354108

Scheerder, A. J., van Deursen, A. J. A. M., & van Dijk, J. A. G. M. (2019). Negative Outcomes of Internet Use: A Qualitative Analysis in the Homes of Families with Different Educational Backgrounds. *The Information Society, 35,* 286-298.

Trauth, E. M., & Jessup, L. M. (2000). Understanding Computer-Mediated Discussions: Positivist and Interpretive Analyses of Group Support System Use. *MIS Quarterly, 24,* 43-79. https://doi.org/10.2307/3250979

Von Solms, B. (2001). Information Security: A Multidimensional Discipline. *Computers & Security, 20,* 504-508. https://doi.org/10.1016/S0167-4048(01)00608-3

Willcocks, L., & Margetts, H. (1994). Risk Assessment and Information Systems. *European Journal of Information Systems, 3,* 127-139. https://doi.org/10.1057/ejis.1994.13